IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

SPYRO STAMAT, individually and on behalf of others similarly situated,	*	
Plaintiff,	*	
v.	*	**Civil Case No.: SAG-22-00747**
GRANDIZIO WILKINS LITTLE & MATTHEWS, LLP,	*	
Defendant.	*	

* * * * * * * * * * * * *

MEMORANDUM OPINION

Plaintiff Spyro Stamat, on behalf of himself and others similarly situated, filed this class action against Defendant Grandizio Wilkins Little & Matthews, LLP ("Grandizio") seeking monetary, declaratory, and injunctive relief for the alleged negligent failure to protect Personal Identifying Information ("PII") from unauthorized access, and for unjust enrichment. ECF 1. Defendant has filed a Motion to Dismiss the Complaint ("Motion"). ECF 16. The issues have been fully briefed, ECF 16-1, 18, 23, and no hearing is necessary. *See* Local Rule 105.6 (D. Md. 2021). For the following reasons, Defendant's Motion will be granted.

I. BACKGROUND

The following facts are derived from the Complaint, ECF 1, and are taken as true for purposes of evaluating Defendant's Motion. Plaintiff, Mr. Stamat, is a resident of Delaware. ECF 1 ¶ 9. Defendant Grandizio, a Maryland corporation, is an accounting firm that offers tax and business services. *Id.* ¶¶ 15–16. Grandizio acquires and stores PII of individuals in connection with its services. *Id.* ¶ 49.

A. The Data Breach

On June 7, 2021, Grandizio discovered unauthorized access into one of its employee's email accounts. ECF 1 ¶ 28. Grandizio commissioned an investigation with cybersecurity experts to determine whether any information had been compromised. *Id.* ¶ 29. The internal investigation completed on December 17, 2021, but could not conclusively determine whether any data has been or will be misused by those who gained unauthorized access to the email account. *Id.* ¶¶ 35, 36. The following month, on or around January 14, 2022, Grandizio informed relevant States' Attorney Generals about the breach of its email account. *Id.* ¶ 38. At the same time, Grandizio sent written notification to any individuals whose data may have been compromised. *Id.* ¶ 39.

Thereafter, Mr. Stamat received a "Notice of Data Security Incident" from Grandizio, *id.* ¶ 9, informing him about the email account breach and noting that some of the company's files "may have been accessed by the unauthorized individual" that "may have contained names, Social Security numbers, Medical Information, Drivers['] License Information, Financial Account Information, or Payment Card Information," *id.* ¶ 31. The letter further informed Mr. Stamat that his personal information "may have been involved." *Id.* The letter offered single bureau credit and identity monitoring services for 12 months, *id.* ¶ 82, and suggested Mr. Stamat take measures to protect against possible identity theft, *id.* ¶ 13.

Mr. Stamat does not purport to have worked with Grandizio directly; he alleges that Grandizio acquired his PII through a third-party intermediary without his knowledge. *Id.* ¶ 21 ("Plaintiff and Class Members were persons who provided, or who third-parties provided on their behalf, their PII to Defendant in conjunction with utilizing [Grandizio's] tax and business services."); ECF 18 at 23 ("[T]his is a situation where Defendant, without Mr. Stamat's knowledge, took control of Mr. Stamat's valuable asset, his PII[.]"). Beyond the information

provided in the letter, Mr. Stamat is unaware to what extent his PII has been compromised (if at all), what type of his information may have been compromised, or how the unauthorized email access occurred. ECF 1 ¶ 30. Mr. Stamat believes the likely mechanism was an email phishing attack of one of Grandizio's employees. *Id.* ¶ 57. Mr. Stamat "further believes his PII, and that of Class Members, was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type." *Id.* ¶ 41.

B. Plaintiff's Injury

As a result of the potential exposure of his PII, Mr. Stamat spends "a considerable amount of time" monitoring his accounts and credit scores and researching how the unauthorized access of the email account may have impacted him. ECF 1 ¶ 105. Mr. Stamat further "anticipates spending considerable time and money on an ongoing basis" to mitigate and prevent potential misuses of his PII. *Id.* ¶ 110. Mr. Stamat has "sustained emotional distress," *id.* ¶ 105, specifically, he has "suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy," *id.* ¶107.

In total, Mr. Stamat alleges that the failure to protect PII from unauthorized access resulted in the following injuries to himself and other similarly situated individuals:

> (i) the current and imminent risk of fraud and identity theft[;]
> (ii) lost or diminished value of PII;
> (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII;
> (iv) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; and
> (v) the continued and certainly increased risk to their PII, which:
> (a) remains unencrypted and available for unauthorized third parties to access and abuse; and
> (b) may remain backed up in Defendant's possession and is subject to further unauthorized disclosures so

long as Defendant fails to undertake appropriate and adequate measures to protect the PII;

(vi) the invasion of privacy;

(vii) the compromise, disclosure, theft, and unauthorized use of Plaintiff's and the Class Members' PII; and

(viii) emotional distress, fear, anxiety, nuisance and annoyance related to the theft and compromise of their PII.

Id. ¶ 6.

C. The Present Case

Mr. Stamat, individually and on behalf of those similarly situated, filed the Class Action Complaint in this Court on March 28, 2022. He purports to represent "[a]ll persons [Grandizio] identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach." *Id.* ¶ 111. Mr. Stamat, and those he represents, allege that Grandizio negligently failed to reasonably secure their PII (Counts I, III) and became unjustly enriched through use of the PII without implementing adequate safeguards (Count II). ECF 1.

Grandizio has now filed a motion to dismiss the Complaint under Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6). ECF 16. Grandizio's Motion is based upon two grounds. First, Grandizio argues that the Court should dismiss Mr. Stamat's Complaint because he has failed to allege an injury-in-fact and lacks standing. Second, Grandizio asserts that the Court should dismiss Mr. Stamat's claims for failure to state a claim upon which relief can be granted. Grandizio's Rule 12(b)(1) Motion will be granted for lack of standing. As a result, the Court will find moot and not address Grandizio's alternative arguments to dismiss under Rule 12(b)(6).

II. LEGAL STANDARDS

A. Rule 12(b)(1) Standard

When a Rule 12(b)(1) motion contests the factual basis for subject matter jurisdiction, the burden of proving subject matter jurisdiction rests with the plaintiff. *Richmond, Fredericksburg*

& Potomac R.R. Co. v. United States, 945 F.2d 765, 768 (4th Cir. 1991). A challenge to jurisdiction may be either facial, *i.e.*, the complaint fails to allege facts upon which subject matter jurisdiction can be based, or factual, *i.e.*, jurisdictional allegations of the complaint are not true. *Adams v. Bain*, 697 F.2d 1213, 1219 (4th Cir. 1982). *See also Kerns v. United States*, 585 F.3d 187, 192 (4th Cir. 2009) (same); *Richmond, Fredericksburg & Potomac R.R. Co.,* 945 F.2d at 768 (same). In determining whether jurisdiction exists, the district court regards the pleadings' allegations as mere evidence and may consider evidence outside the pleadings without converting the proceeding to one for summary judgment. *Richmond, Fredericksburg & Potomac R.R. Co.,* 945 F.2d at 768.

B. Standing for a Class Action Complaint

Article III of the U.S. Constitution limits the jurisdiction of federal courts to "Cases" and "Controversies." U.S. Const. art. III, § 2. "One element of the case-or-controversy requirement is that plaintiffs must establish that they have standing to sue." *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 408 (2013) (internal citations and quotation marks omitted). To invoke federal jurisdiction, a plaintiff bears the burden of establishing the minimum requirements of Article III standing. *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 561 (1992).

"[T]he procedural posture of the case dictates the plaintiff's burden as to standing." *Beck v. McDonald*, 848 F.3d 262, 270 (4th Cir. 2017) (citing *Lujan*, 504 U.S. at 561). "At the pleading stage, general factual allegations of injury resulting from the defendant's conduct may suffice, for on a motion to dismiss we presume that general allegations embrace those specific facts that are necessary to support the claim." *Id.* (quoting *Lujan*, 504 U.S. at 561) (internal quotation marks omitted).

In a class action, "[e]very class member must have Article III standing in order to recover individual damages." *TransUnion LLC v. Ramirez*, __ U.S. __; 141 S. Ct. 2190, 2208 (2021). The Court analyzes standing based on the allegations of personal injury made by the named plaintiffs. *Beck*, 848 F.3d at 269 (citing *Doe v. Obama*, 631 F.3d 157, 160 (4th Cir. 2011)). "Without a sufficient allegation of harm to the named plaintiff in particular, plaintiffs cannot meet their burden of establishing standing." *Id.* at 270 (quoting *Doe*, 631 F.3d at 160) (internal quotation marks omitted).

III. DISCUSSION

To invoke federal jurisdiction, a plaintiff must establish the three "irreducible" minimum requirements of Article III standing: (1) injury-in-fact, (2) causation, and (3) redressability. *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560 (1992). At issue here is the first element—injury-in-fact.

"To establish injury in fact, a plaintiff must show that he or she suffered 'an invasion of a legally protected interest' that is 'concrete and particularized' and 'actual or imminent, not conjectural or hypothetical.'" *Spokeo, Inc. v. Robins*, 578 U.S. 330, 339 (2016) (quoting *Lujan*, 504 U.S. at 560). Although a "'threatened rather than actual injury can satisfy Article III standing requirements,' . . . not all threatened injuries constitute an injury-in-fact." *Beck*, 848 F.3d at 271 (quoting *Friends of the Earth, Inc. v. Gaston Copper Recycling Corp.*, 204 F.3d 149, 160 (4th Cir. 2000)). "Although 'imminence' is concededly a somewhat elastic concept, it cannot be stretched beyond its purpose, which is to ensure that the alleged injury is not too speculative for Article III purposes." *Id.* (quoting *Lujan*, 504 U.S. at 564–65, n.2) (internal quotation marks omitted). Ultimately, a "threatened injury must be *certainly impending* to constitute injury in fact." *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 409 (2013) (internal citations and quotation marks omitted) (emphasis in original).

In his Complaint, Mr. Stamat provides a list of alleged harms—actual and imminent—resulting from the unauthorized email access. Each of these alleged harms is addressed in turn.

A. Imminent Harm

Mr. Stamat identifies the "current and imminent risk of fraud and identity theft" as an injury for standing purposes. ECF 1 ¶ 6. Mr. Stamat urges the Court to "follow the growing number of courts that have found the imminent risk of future harm is a legally cognizable injury." ECF 18 at 7. Grandizio counters that this threat of injury is speculative and insufficient to establish Article III standing. ECF 16-1 at 6.

While circuit courts have splintered on whether the increased risk of identity theft constitutes an Article III injury, Fourth Circuit precedent is relatively straightforward. The Fourth Circuit first addressed this issue in *Beck v. McDonald*, 848 F.3d 262 (4th Cir. 2017). In *Beck*, the Fourth Circuit consolidated two appeals brought by veterans who had received health care at a Veterans Affairs Medical Center ("VA"). *Id.* at 266. In one case, a stolen VA laptop contained unencrypted PII of approximately 7,400 patients, including names, birth dates, the last four digits of Social Security numbers, and physical descriptors (age, race, gender, height, and weight). *Id.* at 267. In the second case, four stolen or misplaced boxes of pathology reports contained PII of over 2,000 patients, including names, Social Security numbers, and medical diagnoses. *Id.* at 268. The VA alerted the affected individuals and offered each of them a year of free credit monitoring. *Id.* Plaintiffs in both cases argued that the increased risk of identity theft following these two incidents constituted an injury-in-fact.

The Fourth Circuit disagreed. It first invoked the Supreme Court's discussion of standing based on "threatened injuries" in *Clapper v. Amnesty International USA*, 568 U.S. 398 (2013). The Fourth Circuit noted that although a future risk of harm, in some cases, can amount to a

concrete imminent harm, *Beck*, 848 F.3d. at 271, a plaintiff must nonetheless satisfy "the Court's long-established requirement that 'threatened injury must be certainly impending to constitute injury in fact,'" *id.* at 272 (citing *Clapper*, 568 U.S. at 1147–48). The Fourth Circuit concluded that the plaintiffs failed to meet this burden because they did not allege any actual misuse of the VA's missing information. *Id.* Moreover, the potential harm of identity theft required an "attenuated chain of possibilities" like the Supreme Court deemed insufficient in *Clapper*, specifically that the data thief targeted the stolen items because they contained PII, that the thief will select the named plaintiff's PII, and the thief will successfully use that information to steal their identities. *Id.* at 275. The Fourth Circuit further rejected the suggestion that the future identity theft itself (rather than the increased risk of such a theft) could establish standing in *Beck*. *Id.* at 276. The plaintiffs provided statistics on health-related data breaches, emphasized that the defendant offered free credit monitoring services, and highlighted the defendant's own admission that a "reasonable risk exists" for the "potential misuse of sensitive personal information." *Id.* However, the Fourth Circuit found none of this evidence to demonstrate a "substantial risk" of identity theft sufficient to confer standing. *Id.*

The Fourth Circuit acknowledged the circuit split on this issue. *Id.* at 273 ("Our sister circuits are divided on whether a plaintiff may establish an Article III injury-in-fact based on an increased risk of future identity theft."). In fact, it reviewed the cases where courts found that the increased risk of identity theft satisfied the injury-in-fact requirement, noting that the plaintiffs in those cases made allegations sufficient to "push the threatened injury of future identity theft beyond the speculative to the sufficiently imminent." *Id.* at 274. Specifically, in some of those cases, the data thief intentionally sought to steal PII, *id.* (citing *Galaria v. Nationwide Mut. Ins. Co.*, 663 F. App'x 384, 386 (6th Cir. 2016), *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688,

694 (7th Cir. 2015), and *Pisciotta v. Old Nat. Bancorp*, 499 F.3d 629, 632 (7th Cir. 2007)), and in others, at least one named plaintiff alleged actual misuse or access of the PII, *id.* (citing *Remijas*, 794 F.3d at 690 and *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1141 (9th Cir. 2010)). In contrast, the Fourth Circuit found the *Beck* plaintiffs' risk of future identity theft was "too speculative" and affirmed the district court's dismissal of the cases for lack of standing. *Beck*, 848 F.3d at 274.

A similar issue arose before the Fourth Circuit the following year in *Hutton v. Nat'l Bd. of Examiners in Optometry, Inc.*, 892 F.3d 613 (4th Cir. 2018). Unlike the plaintiffs in *Beck*, however, the *Hutton* plaintiffs did allege misuse of their stolen personal identity information. The case originated when a group of optometrists from across the United States noticed that Chase Amazon Visa credit card accounts were being opened in their names. *Id.* at 616. The opening of these accounts required PII, including Social Security numbers, names, dates of birth, addresses, and credit card information. *Id.* at 617. These geographically disparate optometrists shared one organization in common: the National Board of Examiners in Optometry ("NBEO"). *Id.* at 617. In addition, Rhonda Hutton, one of the named plaintiffs, specifically received an Amazon Visa credit card that she had never applied for, which was generated using outdated personal information from when she first submitted her data to NBEO. *Id.*

Relying on *Beck*, the district court dismissed the case for lack of standing, but the Fourth Circuit disagreed. *Id.* at 616. The Fourth Circuit re-emphasized "that that a mere compromise of personal information, without more, fails to satisfy the injury-in-fact element in the absence of an identity theft." *Id.* at 621. But the Fourth Circuit distinguished *Beck*, explaining:

> In *Beck*, the plaintiffs alleged only a threat of future injury in the data breach context where a laptop and boxes—containing personal information concerning patients, including partial social security numbers, names, dates of birth, and physical descriptions—had been stolen, but the information contained therein had not been misused. The Plaintiffs in these cases, on the other hand, allege that they have

> already suffered actual harm in the form of identity theft and credit card fraud.

Id. at 621–22. In contrast to *Beck*, the *Hutton* plaintiffs had examples of fraudulent credit cards taken out in their names and at least one named plaintiff noted that her credit score fell by eleven points because of a fraudulent application. *Id.* at 622. Thus, the Fourth Circuit concluded that the plaintiffs' allegations of actual misuse of the stolen personal information satisfied the Article III standing requirements of a concrete injury. *Id.* at 622.

The Fourth Circuit further noted that "[a]t a minimum, Plaintiffs have sufficiently alleged an imminent threat of injury to satisfy Article III standing" given the plaintiffs alleged that their data had been used in a fraudulent manner. *Id.* Thus, the Fourth Circuit considered mitigation costs incurred by the plaintiffs, such as costs of credit monitoring services and time lost notifying credit reporting agencies about the data breach, to establish an injury-in-fact for Article III standing. In contrast to any preemptive mitigation efforts taken by the plaintiffs in *Beck*, the mitigation efforts by the plaintiffs in *Hutton* were in response to a substantial and sufficiently imminent risk of identity theft, as evinced by the existing misuse of their data. *Id.* Cases following *Hutton* have generally found plaintiffs to establish standing when they show actual misuse of the stolen data. *See, e.g.*, *In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 459 (D. Md. 2020) (complaint "contains allegations of actual misuse by some of the plaintiffs"); *Bank of Louisiana v. Marriott Int'l, Inc.*, 438 F. Supp. 3d 433, 440 (D. Md. 2020) (complaint alleges that "payment card information actually has been accessed, and used in a fraudulent manner"); *McCreary v. Filters Fast LLC*, No. 3:20-CV-595-FDW-DCK, 2021 WL 3044228, at *5 (W.D.N.C. July 19, 2021) (complaint alleged the misuse of their credit cards through fraudulent charges and publication of the information on the Dark Web). In contrast, like in *Beck,* courts frequently dismiss cases for lack of standing when the plaintiffs fail to show any

resulting misuse of their data. *See, e.g.*, *Kimbriel v. ABB, Inc.*, No. 5:19-CV-215-BO, 2019 WL 4861168, at *3 (E.D.N.C. Oct. 1, 2019) (plaintiffs merely alleged their information was used to conduct a credit inquiry); *Krohm v. Epic Games, Inc.*, 408 F. Supp. 3d 717, 720 (E.D.N.C. 2019) ("plaintiff's complaint contains no facts showing, or even suggesting, that his personal data has been used as a result of the cyber vulnerability").

In the present case, Mr. Stamat alleges no actual misuse of his personal data. He does not provide any instance where his personal information has been fraudulently used to open a credit card, make fraudulent charges, or used in such a way to lower his credit score. All potential harms and misuses of his data remain hypothetical.

Actual misuse of data, however, is not strictly required to establish standing in the data breach context. In other circuits, courts have permitted a plaintiff to establish standing where the PII was the specific target of the attack. *See, e.g.*, *Galaria v. Nationwide Mut. Ins. Co.*, 663 F. App'x 384, 388 (6th Cir. 2016) ("Where a data breach targets personal information, a reasonable inference can be drawn that the hackers will use the victims' data for the fraudulent purposes alleged in Plaintiffs' complaints."). Assuming such an argument would succeed in the Fourth Circuit, which has not yet addressed the precise issue, Mr. Stamat's allegations nonetheless fall short. In contrast to cases where a hacker targets a database of PII or specifically accesses PII during a cyber attack, Mr. Stamat has only alleged that an email account was accessed by an unauthorized user, and that this email account may have included some of his PII. There is no reason to suggest that the PII accessible in the email account was the specific target of the attack. Thus, Mr. Stamat relies on an attenuated chain of possibilities with no alleged facts to support them: that his PII was the target of the attack, that the unauthorized user actually accessed his PII, and that the user will successfully misuse his data to commit identity theft and fraud. Without

allegations of existing misuse, the potential for fraudulent use of Mr. Stamat's PII remains too speculative to confer an imminent injury.

Finally, Mr. Stamat also points to the "continued and certainly increased risk" to his PII that remains stored in Grandizio's possession. But this too does not amount to "certainly impending" or concrete harm. The Fourth Circuit has explained that the "mere compromise of personal information, without more, fails to satisfy the injury-in-fact element in the absence of an identity theft." *Hutton v. Nat'l Bd. of Examiners in Optometry, Inc.*, 892 F.3d 613, 621 (4th Cir. 2018) (citing *Beck*, 848 F.3d at 274–75). Thus, even assuming that Grandizio maintains PII inadequately in the general course, because even the actual data breach fails to establish injury-in-fact, any continued risk of another data breach is equally unsatisfactory for Article III standing purposes.

B. Actual Harm

In addition to the risk of future harm, Mr. Stamat identifies various actual harms he alleges he has suffered as a result of Grandizio's failure to adequately protect his PII from unauthorized access.

First, Mr. Stamat points to the unauthorized access itself and the resulting "invasion of privacy." ECF 1 ¶ 6. Specifically, he lists the "compromise, disclosure, theft, and unauthorized use of Plaintiff's and the Class Members' PII" as alleged injuries. *Id.* But as noted above, the mere potential compromise of personal information does not amount to a concrete harm for constitutional standing purposes. *Hutton*, 892 F.3d at 621. The fact that an unauthorized third party accessed the email account of a Grandizio employee, which may have contained Mr. Stamat's PII, does not on its own provide an actionable injury or show that his privacy was invaded.

Next, Mr. Stamat points to the "lost or diminished value" of his PII. ECF 1 ¶ 6. Such an economic loss in value could be recognizable as a concrete injury. However, Mr. Stamat fails to allege any support for the proposition that his or any class member's PII lowered in value because of the data breach. Rather, he presents research on how much others would likely pay for his stolen information, estimating a range from between $50 to $200, depending on the type of credential. *Id.* ¶ 66. The fact that someone else can profit from having access to his information does not necessarily lower the value of that information to Mr. Stamat. Indeed, the misuse of PII can damage its value and lower Mr. Stamat's credit scores, but until that misuse occurs, Mr. Stamat has not been concretely harmed.

Additionally, Mr. Stamat alleges that he experiences "emotional distress, fear, anxiety, nuisance and annoyance related to the theft and compromise of their PII." *Id.* ¶ 6. Emotional injuries may suffice for Article III standing purposes. *See TransUnion LLC v. Ramirez*, __ U.S. __; 141 S. Ct. 2190, 2211 n.7 (2021) ("[A] plaintiff's knowledge that he or she is exposed to a risk of future physical, monetary, or reputational harm could cause its own current emotional or psychological harm. We take no position on whether or how such an emotional or psychological harm could suffice for Article III purposes[.]"). However, as emphasized in *Beck*, "bare assertions of emotional injury" are insufficient to confer Article III standing. *Beck*, 848 F.3d at 273 (citing *Doe v. Chao*, 540 U.S. 614, 624–25 (2004)). Thus, the Fourth Circuit rejected the plaintiffs' claim that "emotional upset" and "fear [of] identity theft and financial fraud" resulting from the data breaches were "adverse effects" sufficient to confer Article III standing. *Beck*, 848 F.3d at 272. Here, Mr. Stamat alleges nothing more than similarly bare assertions of emotional harm. He merely states that he has "sustained emotional distress" and "suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased

concerns for the loss of his privacy," without alleging any facts to support these assertions. ECF 1 ¶¶ 105, 107. Thus, his alleged emotional injuries do not amount to a concrete harm.

Finally, Mr. Stamat raises multiple examples of mitigation efforts he voluntarily undertook to prevent future identity theft and fraud. He identifies the "out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII" and the "lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time." ECF ¶ 6. All of these may be actual harms in certain circumstances. In the context of this case, though, Mr. Stamat's actions constitute self-imposed mitigation measures to protect against a non-imminent harm. *See Beck*, 848 F.3d at 276–77 (rejecting plaintiffs' similar argument that the costs incurred to guard against identity theft, including the cost of credit monitoring services and the burden of self-monitoring their credit, constituted an injury-in-fact because the harm was non-imminent).

It is not out of the realm of possibility that other individuals in the proposed class have suffered some concrete harm as a result of the unauthorized email access, if there has been actual misuse of their PII. But the Complaint fails to provide examples of misuse of any other plaintiffs' information, and for the purposes of determining standing for a class action complaint, the Court reviews Mr. Stamat's alleged injuries as the named plaintiff. *See Beck*, 848 F.3d at 269 (citing *Doe v. Obama*, 631 F.3d 157, 160 (4th Cir. 2011)). As discussed, Mr. Stamat has failed to allege any concrete harm—imminent or actual—to establish injury-in-fact for Article III standing.

IV. CONCLUSION

For the reasons set forth above, Grandizio's Motion to Dismiss, ECF 16, is granted. A separate Order follows.

Dated: August 31, 2022

/s/
Stephanie A. Gallagher
United States District Judge